UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,433	02/06/2004	Marcus Leech	57983.000164	5978

7590 10/22/2009

Thomas E. Anderson
Hunton & Williams LLP
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/772,433	LEECH, MARCUS	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 0209*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-20* is/are pending in the application.

4a) Of the above claim(s) *1 and 3-11* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 16 July 2009 amends claims 1, 12. Applicant's amendment has been fully considered and entered.

Election/Restrictions

2. This application contains claims 1, 3-11 drawn to an invention nonelected with traverse. A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

Response to Arguments

3. Applicant argues, "Applicant is unable to provisionally elect a species as the Examiner has made a constructive election and therefore not afforded Applicant that option." In response, Examiner would like to point out that Applicant provisionally elected species 1 by original presentation. Identified species 1 involves an embodiment of the invention that utilizes first and second masks that are the same value. Identified species 2 involves a different embodiment of the invention that utilizes first and second masks that are not the same value. The original claims only included claims belonging to identified species 1. If Applicant had filed original claims that included both species, Applicant would have been given the opportunity to provisionally elect prior to receiving action on the merits. However, because the originally presented claims only included claims belonging to identified species 1, Applicant constructively elected species 1 by original presentation.

4. Applicant argues, "Examiner restricts originally filed claim 5 from claim 1...by definition, it is not independent...the restriction requirement is improper and Applicant

respectfully requests withdraw of the same." The argument is not persuasive because the Examiner did not restrict "originally filed claim 5 from claim 1", but instead restricted the embodiment of invention characterized by originally filed claim 5 from the embodiment of invention characterized by current claims 1, 3-11.

5. Applicant argues, "The restriction requirement is additionally improper because it lists two species and includes a generic claim in one of the species. A claim cannot be a genus and a species at the same time." In response, the Examiner did not identify any generic claims. Therefore, Applicant's argument is unpersuasive.

6. Applicant argues, "The restriction requirement is also incomprehensible. Claim 5 is included in both species." In response, Examiner would like to reiterate that the embodiment of invention characterized by originally filed claim 5 is restricted from the embodiment of invention characterized by current claims 1, 3-11.

7. Applicant argues, "The restriction requirement…is improper because the Examiner withdrew from consideration claims 1 and 3-11 without consent from the Applicant." In response, no consent was required because Applicant received an action on the merits for the originally presented species.

8. Applicant argues, "No new claims have been added. Thus, this situation does not exist here." This argument is not persuasive because the claim language representative of species 2 was added by amendment (19 December 2007) following action by the Examiner (18 June 2007).

9. Applicant's arguments, with respect to §101 rejections of claims 12-19 have been fully considered and are persuasive. The §101 rejections of claims 12-19 have been withdrawn.

10. Applicant argues, "Rogaway does not disclose any function that could be analogized to the presently claimed application of an XOR function to all message blocks of a message." This argument is not persuasive because the algorithm depicted by Rogaway on page 5 clearly shows that each message block (M[i]) is XOR'd with the value Z[i].

11. Applicant argues, "Further, Rogaway fails to disclose, or even suggest, any value that could be analogized to the presently claimed XOR-sum." This argument is not persuasive because the result of the checksum calculation could be considered an XOR-sum. Additionally, the computation of C can be considered an XOR-sum.

12. Applicant argues, "A concatenation operation is very different from an XOR operation in both form and result." In response, Examiner never suggested that the concatenation was equivalent to the claimed XOR function, but instead was equivalent to the summation operation. Rogaway discloses concatenating a plurality of XOR'd values (Page 5), which is equivalent to the claimed XOR-sum.

13. Applicant argues, "Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block cipher E, as well as applying the same message string M[m} after the block cipher E…applying an offset Z[m] to a checksum before a block cipher E, and then limiting the block cipher result to a tag length t…This disclosure by Rogaway clearly differs from the claimed invention." Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway, in view of Schneier. Referring to claims 12, 20, Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask value to the XOR-sum. The result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

Referring to claim 13, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first/third mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second/fourth mask value is computed by applying a XOR function to a fourth value derived from the nonce value and a fifth value derived from encrypting a sixth value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt M[i] ⊕ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 14, Rogaway discloses that to compute the R value, the nonce is XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets

the limitation of the first and fourth values derived from the nonce value are permutations of a binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claims 15, 16, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, M[i] ⊕ Z[i]), which meets the limitation of whitening at least one message block with a third mask value. The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which meets the limitation of encrypting the at least one whitened message block using a block cipher and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of whitening the at least one encrypted message block with the third mask value to generate at least one corresponding output ciphertext block.

Referring to claim 17, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first and second mask values are computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt M[i] ⊕ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that

is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 18, Rogaway discloses that the block cipher used is the AES block cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Referring to claim 19, Rogaway discloses that the L and R values are elements of the offset vector Z (page 5), which meets the limitation of the second and fifth values are elements of a vector.

Conclusion

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432